#2
12/14/01

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Katsuya SHINOHARA

Serial No. (unknown)

Filed herewith

CHAINING KEY BROADCASTING RECEPTION SYSTEM AND
CHAINING KEY BROADCASTING RECEPTION METHOD

CLAIM FOR FOREIGN PRIORITY UNDER 35 U.S.C. 119
AND SUBMISSION OF PRIORITY DOCUMENT

Assistant Commissioner for Patents

Washington, D.C. 20231

Sir:

Attached hereto is a certified copy of applicant's corresponding patent application filed in Japan under 2000-355123, filed on 22 November 2000.

Applicant herewith claims the benefit of the priority filing date of the above-identified application for the above-entitled U.S. application under the provisions of 35 U.S.C. 119.

Respectfully submitted,

YOUNG & THOMPSON

By Benoît Castel

Benoît Castel
Attorney for Applicant
Customer No. 000466
Registration No. 35,041
745 South 23rd Street
Arlington, VA 22202
703/521-2297

November 20, 2001

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application: ２０００年１１月２２日

出 願 番 号
Application Number: 特願２０００－３５５１２３

出 願 人
Applicant(s): 日本電気株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年 ８月３１日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及川耕造

【書類名】　特許願
【整理番号】　68501895
【提出日】　平成12年11月22日
【あて先】　特許庁長官殿
【国際特許分類】　G09C　1/00
【発明者】
　【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
　【氏名】　篠原　克也
【特許出願人】
　【識別番号】　000004237
　【氏名又は名称】　日本電気株式会社
【代理人】
　【識別番号】　100088812
　【弁理士】
　【氏名又は名称】　▲柳▼川　信
【手数料の表示】
　【予納台帳番号】　030982
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9001833
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　連鎖鍵放送受信システム及び連鎖鍵放送受信方法

【特許請求の範囲】

【請求項１】　ディジタル放送を受信するための連鎖鍵放送受信システムであって、前記ディジタル放送における複数の番組を視聴した時に得られる鍵情報に基づいて予め暗号化されたコンテンツを復号化するための鍵情報を得る手段を有することを特徴とする連鎖鍵放送受信システム。

【請求項２】　前記鍵情報を得る手段は、前記コンテンツを復号化するための連鎖鍵とその鍵識別子とその鍵が復号化する連鎖鍵を示す対象鍵識別子とを受信する連鎖鍵受信手段と、前記対象鍵識別子を用いて既に保存されている連鎖鍵を取出す連鎖鍵保存手段と、前記連鎖鍵保存手段から送られてくる連鎖鍵を用いて前記連鎖鍵受信手段が受信した連鎖鍵を復号化して新たな連鎖鍵を生成する連鎖鍵復号化手段とを含むことを特徴とする請求項１記載の連鎖鍵放送受信システム。

【請求項３】　前記連鎖鍵の受信と復号化と保存との一連の処理と、その連鎖鍵を用いる処理とを独立して実行するよう構成したことを特徴とする請求項２記載の連鎖鍵放送受信システム。

【請求項４】　前記連鎖鍵を用いる処理が暗号化コンテンツの復号化処理であることを特徴とする請求項３記載の連鎖鍵放送受信システム。

【請求項５】　任意の連鎖鍵の識別子を前記対象識別子として指定するようにしたことを特徴とする請求項１から請求項４のいずれか記載の連鎖鍵放送受信システム。

【請求項６】　ディジタル放送を受信するための連鎖鍵放送受信方法であって、前記ディジタル放送における複数の番組を視聴した時に得られる鍵情報に基づいて予め暗号化されたコンテンツを復号化するための鍵情報を得るステップを有することを特徴とする連鎖鍵放送受信方法。

【請求項７】　前記鍵情報を得るステップは、前記コンテンツを復号化するための連鎖鍵とその鍵識別子とその鍵が復号化する連鎖鍵を示す対象鍵識別子と

を受信するステップと、前記対象鍵識別子を用いて既に保存されている連鎖鍵を取出すステップと、その取出された連鎖鍵を用いて受信した連鎖鍵を復号化して新たな連鎖鍵を生成するステップとを含むことを特徴とする請求項６記載の連鎖鍵放送受信方法。

【請求項８】　前記連鎖鍵の受信と復号化と保存との一連の処理と、その連鎖鍵を用いる処理とを独立して実行するようにしたことを特徴とする請求項７記載の連鎖鍵放送受信方法。

【請求項９】　前記連鎖鍵を用いる処理が暗号化コンテンツの復号化処理であることを特徴とする請求項８記載の連鎖鍵放送受信方法。

【請求項１０】　任意の連鎖鍵の識別子を前記対象識別子として指定するようにしたことを特徴とする請求項６から請求項９のいずれか記載の連鎖鍵放送受信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は連鎖鍵放送受信システム及び連鎖鍵放送受信方法に関し、特に暗号鍵を用いてデスクランブルされるディジタル放送におけるスクランブル放送の受信方法に関する。

【０００２】

【従来の技術】

従来、鍵放送システムとしては、ディジタル放送におけるスクランブル放送をデスクランブルするための暗号鍵を受信して復号するために、ＣＡＳ（Ｃｏｎｄｉｔｉｏｎａｌ　Ａｃｃｅｓｓ　Ｓｙｓｔｅｍ：限定受信）カードを用いるものがある。

【０００３】

このＣＡＳカードの処理は、図６に示すように、作業鍵復号化モジュール２３が番組に先立って放送されてくる暗号化されている作業鍵をＣＡＳカード内のマスタ鍵２４を用いて復号化して作業鍵記憶部２１に格納する。

【０００４】

スクランブル鍵復号化モジュール２２は番組と同時に放送されてくる暗号化されているスクランブル鍵を当該作業鍵記憶部２１に格納された作業鍵を用いて復号化してカード外に出力する。尚、図示していないが、ＣＡＳカードの外ではスクランブルされている番組映像をスクランブル鍵を用いて復号化して表示している。

【０００５】

【発明が解決しようとする課題】

上述した従来の鍵放送システムでは、一つの番組の中でスクランブル鍵の復号化のために毎回同じ作業鍵を用いているため、予め作業鍵を入手しておけば、番組放送時には途中から視聴しても、また途中で視聴を一時中断しても、スクランブル鍵を生成することができるので、番組の最初から最後まで視聴した視聴者だけが鍵を使えるようにするといったサービスを実施することができないという問題がある。

【０００６】

また、暗号化されているスクランブル鍵を受信すると、復号化したスクランブル鍵を出力してしまうため、暗号化されているスクランブル鍵の受信と復号化したスクランブル鍵の利用とを非同期に行うことができないという問題がある。

【０００７】

さらにまた、作業鍵の保管とスクランブル鍵の出力とが全く別処理であるため、復号化したスクランブル鍵を次回以降のスクランブル鍵の復号化に用いる作業鍵として用いることができないという問題がある。

【０００８】

そこで、本発明の目的は上記の問題点を解消し、復号化した鍵を次回以降の復号に用いる処理を実現することができる連鎖鍵放送システム及び連鎖鍵放送方法を提供することにある。

【０００９】

【課題を解決するための手段】

本発明による連鎖鍵放送システムは、ディジタル放送を受信するための連鎖鍵放送受信システムであって、前記ディジタル放送における複数の番組を視聴した

時に得られる鍵情報に基づいて予め暗号化されたコンテンツを復号化するための鍵情報を得る手段を備えている。

【００１０】

本発明による連鎖鍵放送方法は、ディジタル放送を受信するための連鎖鍵放送受信方法であって、前記ディジタル放送における複数の番組を視聴した時に得られる鍵情報に基づいて予め暗号化されたコンテンツを復号化するための鍵情報を得るステップを備えている。

【００１１】

すなわち、本発明の連鎖鍵放送システムは、放送を受信する装置において複数の番組を視聴することによって、暗号化コンテンツを解く鍵を得ることができるようにしたことにある。

【００１２】

より具体的に、本発明の連鎖鍵放送システムは、連鎖鍵とその鍵識別子とその鍵が復号化する連鎖鍵を示す対象鍵識別子とを受信する連鎖鍵受信手段と、対象鍵識別子を用いて既に保存されている連鎖鍵を取出す連鎖鍵保存手段と、連鎖鍵保存手段から送られてくる連鎖鍵を用いて連鎖鍵受信手段が受信した連鎖鍵を復号化して新たな連鎖鍵を生成する連鎖鍵復号化手段とを有している。

【００１３】

上記のような構成を採用することによって、一連の連鎖鍵を全て受信しないと最終的な連鎖鍵の復号化ができないという仕組みを実現することが可能となり、放送事業者が自番組を最初から最後まで視聴した、または自放送局の連続番組を欠かさず視聴した視聴者だけが最終的な連鎖鍵を入手することができるようなサービスを実施することが可能となる。例えば、番組Ａと番組Ｂとを視聴した人が連鎖鍵Ｂを、番組Ａと番組Ｃとを視聴した人が連鎖鍵Ｃをそれぞれ得られるというサービスが実現可能となる。

【００１４】

【発明の実施の形態】

次に、本発明の実施の形態について図面を参照して説明する。図１は本発明の実施の形態による連鎖鍵放送システムの構成を示すブロック図である。図１にお

いて、本発明の実施の形態による連鎖鍵放送システムは連鎖鍵受信手段１と、連鎖鍵復号化手段２と、連鎖鍵保存手段３とから構成されている。

【００１５】

連鎖鍵受信手段１は連鎖鍵、その鍵識別子、及びその鍵が復号化する連鎖鍵を示す対象鍵識別子を受信する。連鎖鍵保存手段３は連鎖鍵受信手段１で受信した対象鍵識別子を用いて既に保存されている連鎖鍵を取出す。連鎖鍵復号化手段２は連鎖鍵保存手段３から送られてくる連鎖鍵を用いて、連鎖鍵受信手段１が受信した連鎖鍵を復号化して新たな連鎖鍵を生成する。

【００１６】

これによって、一連の連鎖鍵を全て受信しないと最終的な連鎖鍵の復号化ができないという仕組みを実現することができ、放送事業者が自番組を最初から最後まで視聴した、または自放送局の連続番組を欠かさず視聴した視聴者だけが最終的な連鎖鍵を入手することができるようなサービスを実施することができる。

【００１７】

図２は本発明の一実施例による連鎖鍵放送システムの構成を示すブロック図である。図２において、本発明の一実施例による連鎖鍵放送システムはデマックス１１と、映像デコーダ１２と、映像モニタ１３と、連鎖鍵ハンドラ１４と、連鎖鍵復号化モジュール１５と、連鎖鍵管理モジュール１６と、コンテンツ復号化モジュール１７と、連鎖鍵メモリ１８と、ハードディスク１９とから構成されている。

【００１８】

デマックス１１はディジタル放送信号を受信し、そのディジタル放送信号を動画・音声といったＭＰＥＧ（Ｍｏｖｉｎｇ　Ｐｉｃｔｕｒｅ　Ｅｘｐｅｒｔｓ　Ｇｒｏｕｐ）データと、暗号化連鎖鍵と、鍵識別子と、対象鍵識別子とに分離する。

【００１９】

映像デコーダ１２はＭＰＥＧデータをデコードして映像データを生成する。映像モニタ１３は映像デコーダ１２が生成した映像データをモニタ（図示せず）に表示・再生する。

【００２０】

連鎖鍵管理モジュール１６は連鎖鍵ハンドラ１４から鍵識別子と暗号化連鎖鍵とを受取ると、暗号化連鎖鍵を連鎖鍵として識別子と対にして連鎖鍵メモリ１８に記録し、連鎖鍵ハンドラ１４から対象鍵識別子を受取ると、連鎖鍵メモリ１８内で対象鍵識別子と対になっている連鎖鍵を連鎖鍵復号化モジュール１５に送出する。

【００２１】

また、連鎖鍵管理モジュール１６は連鎖鍵復号化モジュール１５から鍵識別子と連鎖鍵とを受取ると、それらを対にして連鎖鍵メモリに記録し、コンテンツ復号化モジュール１７から鍵識別子を受取ると、連鎖鍵メモリ１８内で鍵識別子と対になっている連鎖鍵をコンテンツ復号化モジュール１７に戻す。

【００２２】

連鎖鍵ハンドラ１４はデマックス１１から暗号化連鎖鍵と鍵識別子と対象鍵識別子とを受取る。連鎖鍵ハンドラ１４は対象鍵識別子がヌルの場合、暗号化連鎖鍵が一連の最初の連鎖鍵であるとして、鍵識別子とともに連鎖鍵管理モジュール１６に送出する。また、連鎖鍵ハンドラ１４は対象鍵識別子がヌルではない場合、２番目以降の暗号化連鎖鍵であるとして、対象鍵識別子を連鎖鍵管理モジュール１６に送出し、暗号化連鎖鍵と鍵識別子とを連鎖鍵復号化モジュール１５に送出する。

【００２３】

連鎖鍵復号化モジュール１５は連鎖鍵管理モジュール１６から受取った連鎖鍵を用いて、暗号化連鎖鍵を復号化し、新たな連鎖鍵を得て、鍵識別子とともに連鎖鍵管理モジュール１６に送出する。

【００２４】

コンテンツ復号化モジュール１７は連鎖鍵管理モジュール１６に鍵識別子を送出し、連鎖鍵管理モジュール１６から得た連鎖鍵を用いてハードディスク１９内の暗号化コンテンツを復号化して目的のコンテンツ（復号化コンテンツ）を得る。ハードディスク１９には予め放送や通信、配布媒体等を経由して入手した暗号化コンテンツが保存されている。

【００２５】

図３は図２の連鎖鍵メモリ１８の構成を示す図である。図３において、連鎖鍵メモリ１８には鍵識別子＃ｎ（ｎ＝１，２，３，４，５，…）と、鍵識別子＃ｎと対の連鎖鍵＃ｎとが格納されている。

【００２６】

図４は本発明の一実施例による連鎖鍵放送システムの連鎖鍵生成処理を示すフローチャートである。これら図２～図４を参照して本発明の一実施例による連鎖鍵放送システムの連鎖鍵生成処理について説明する。本発明の一実施例による連鎖鍵放送システムでは連鎖鍵ハンドラ１４と連鎖鍵管理モジュール１６と連鎖鍵復号化モジュール１６とによって連鎖鍵が順次生成される。

【００２７】

暗号化連鎖鍵、その鍵識別子、及び対象鍵識別子が連鎖鍵ハンドラ１４に与えられると（図４ステップＳ１）、連鎖鍵ハンドラ１４は対象鍵識別子を判定し、対象鍵識別子がヌルであれば（図４ステップＳ２）、鍵識別子と暗号化連鎖鍵とを連鎖鍵管理モジュール１６に送付し、連鎖鍵管理モジュール１６がこれらを対にして連鎖鍵メモリ１８に格納する（図４ステップＳ７）。

【００２８】

連鎖鍵ハンドラ１４は対象鍵識別子がヌルでなければ（図４ステップＳ２）、次のように暗号化連鎖鍵から新たな連鎖鍵を得て、連鎖鍵管理モジュール１６がそれらを連鎖鍵メモリ１８に格納する（図４ステップＳ６）。

【００２９】

暗号化連鎖鍵から新たな連鎖鍵を得る手順は、まず連鎖鍵ハンドラ１４が対象鍵識別子を連鎖鍵管理モジュール１６に送り、連鎖鍵管理モジュール１６がその対の連鎖鍵を連鎖鍵復号化モジュール１５に送出する（図４ステップＳ３）。同時に、連鎖鍵ハンドラ１４は鍵識別子と暗号化連鎖鍵とを連鎖鍵復号化モジュール１５に送出する（図４ステップＳ４）。

【００３０】

連鎖鍵復号化モジュール１５は連鎖鍵ハンドラ１４が得た暗号化連鎖鍵を、連鎖鍵管理モジュール１６から得た連鎖鍵で復号化し、新たな連鎖鍵を得る（図４

ステップＳ５）。連鎖鍵復号化モジュール１５は新たな連鎖鍵と連鎖鍵管理モジュール１６から得た鍵識別子とを連鎖鍵管理モジュール１６に送出し、連鎖鍵管理モジュール１６はこれらを対にして連鎖鍵メモリ１８に格納する（図４ステップＳ６）。

【００３１】

図５は本発明の一実施例による連鎖鍵放送システムの暗号化コンテンツの復号化処理を示すフローチャートである。これら図２と図３と図５とを参照して本発明の一実施例による連鎖鍵放送システムの暗号化コンテンツの復号化処理について説明する。本発明の一実施例による連鎖鍵放送システムではコンテンツ復号化モジュール１７及び連鎖鍵管理モジュール１６によって、連鎖鍵を用いて暗号化コンテンツを復号化している。

【００３２】

この場合、コンテンツ復号化モジュール１７は鍵識別子を指定して連鎖鍵管理モジュール１６から連鎖鍵を取出す（図５ステップＳ１１）。コンテンツ復号化モジュール１７は連鎖鍵管理モジュール１６から得た連鎖鍵を用いて暗号化コンタンツを復号化する（図５ステップＳ１２）。

【００３３】

このように、前回に受信した鍵で次に受信した鍵を順次復号化することによって、番組を最初から最後まで視聴したり、連続ドラマを全回視聴したりして一連の鍵を全て受信した視聴者だけが最終的な鍵を得ることができる。例えば、所望のコンテンツを復号化して入手できるような放送サービスを実現することができる。

【００３４】

また、連鎖鍵の受信・復号化・保存の一連の処理と、その連鎖鍵を用いる処理、例えば暗号化コンテンツの復号化処理とを独立して実施させることによって、連鎖鍵の受信・復号化・保存を行っていない時（例えば、番組を視聴していない時）でも、鍵を用いて蓄積媒体等に保存された暗号化コンテンツを復号化することができる。

【００３５】

さらに、任意の連鎖鍵の識別子を対象識別子として指定することによって、必ずしも連鎖鍵を順番に放送する必要はなく、例えば番組Ａで連鎖鍵Ａを放送し、番組Ｂで送る連鎖鍵Ｂの対象鍵識別子を連鎖鍵Ａ、番組Ｃで送る連鎖鍵Ｃの対象鍵識別子も同じく連鎖鍵Ａとすることで、番組Ａと番組Ｂとを視聴した人は連鎖鍵Ｂを、番組Ａと番組Ｃとを視聴した人は連鎖鍵Ｃを得ることができるといったサービスを柔軟に実施することができる。したがって、復号化した鍵を次回以降の復号に用いる処理を実現することができる。

【００３６】

【発明の効果】

以上説明したように本発明によれば、ディジタル放送を受信するための連鎖鍵放送受信システムにおいて、ディジタル放送における複数の番組を視聴した時に得られる鍵情報に基づいて予め暗号化されたコンテンツを復号化するための鍵情報を得ることによって、復号化した鍵を次回以降の復号に用いる処理を実現することができるという効果がある。

【図面の簡単な説明】

【図１】

本発明の実施の形態による連鎖鍵放送システムの構成を示すブロック図である。

【図２】

本発明の一実施例による連鎖鍵放送システムの構成を示すブロック図である。

【図３】

図２の連鎖鍵メモリの構成を示す図である。

【図４】

本発明の一実施例による連鎖鍵放送システムの連鎖鍵生成処理を示すフローチャートである。

【図５】

本発明の一実施例による連鎖鍵放送システムの暗号化コンテンツの復号化処理を示すフローチャートである。

【図６】

従来例による鍵放送システムの構成を示すブロック図である。

【符号の説明】

１　連鎖鍵受信手段

２　連鎖鍵復号化手段

３　連鎖鍵保存手段

１１　デマックス

１２　映像デコーダ

１３　映像モニタ

１４　連鎖鍵ハンドラ

１５　連鎖鍵復号化モジュール

１６　連鎖鍵管理モジュール

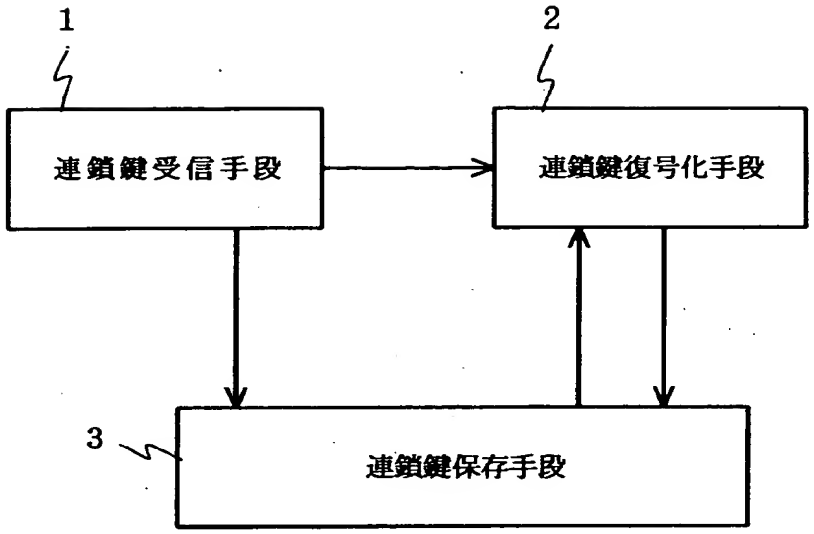
１７　コンテンツ復号化モジュール

１８　連鎖鍵メモリ

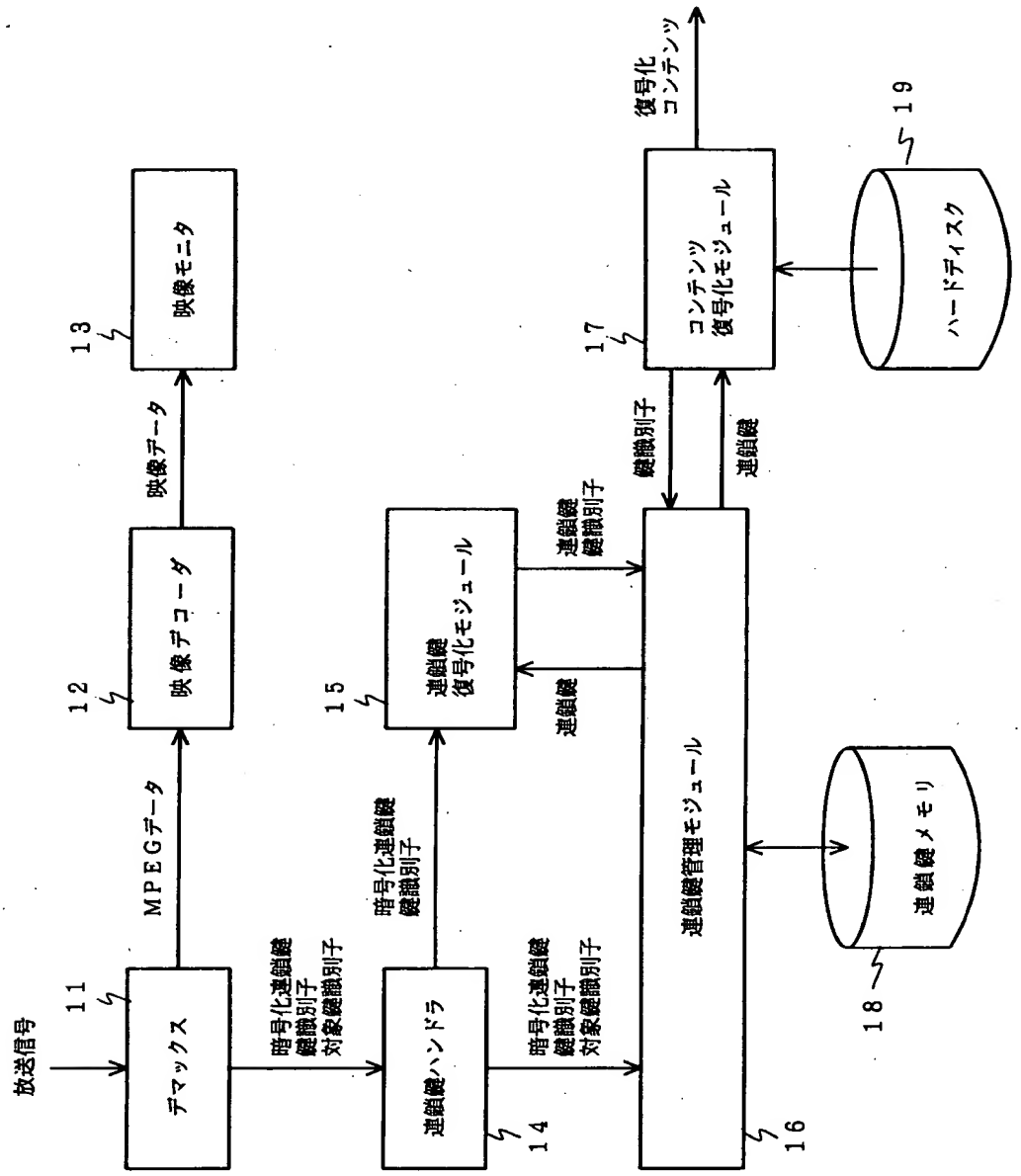
１９　ハードディスク

【書類名】　　図面

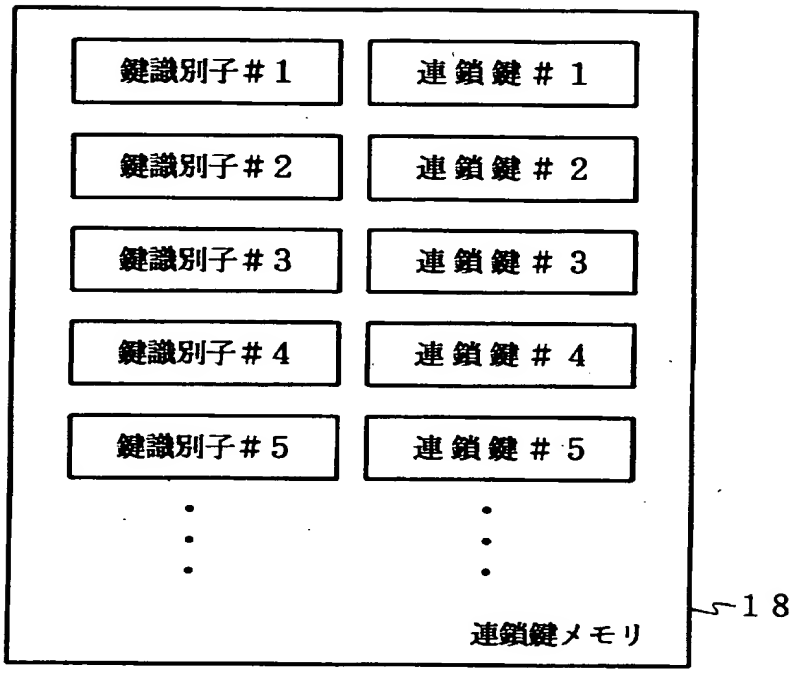
【図１】



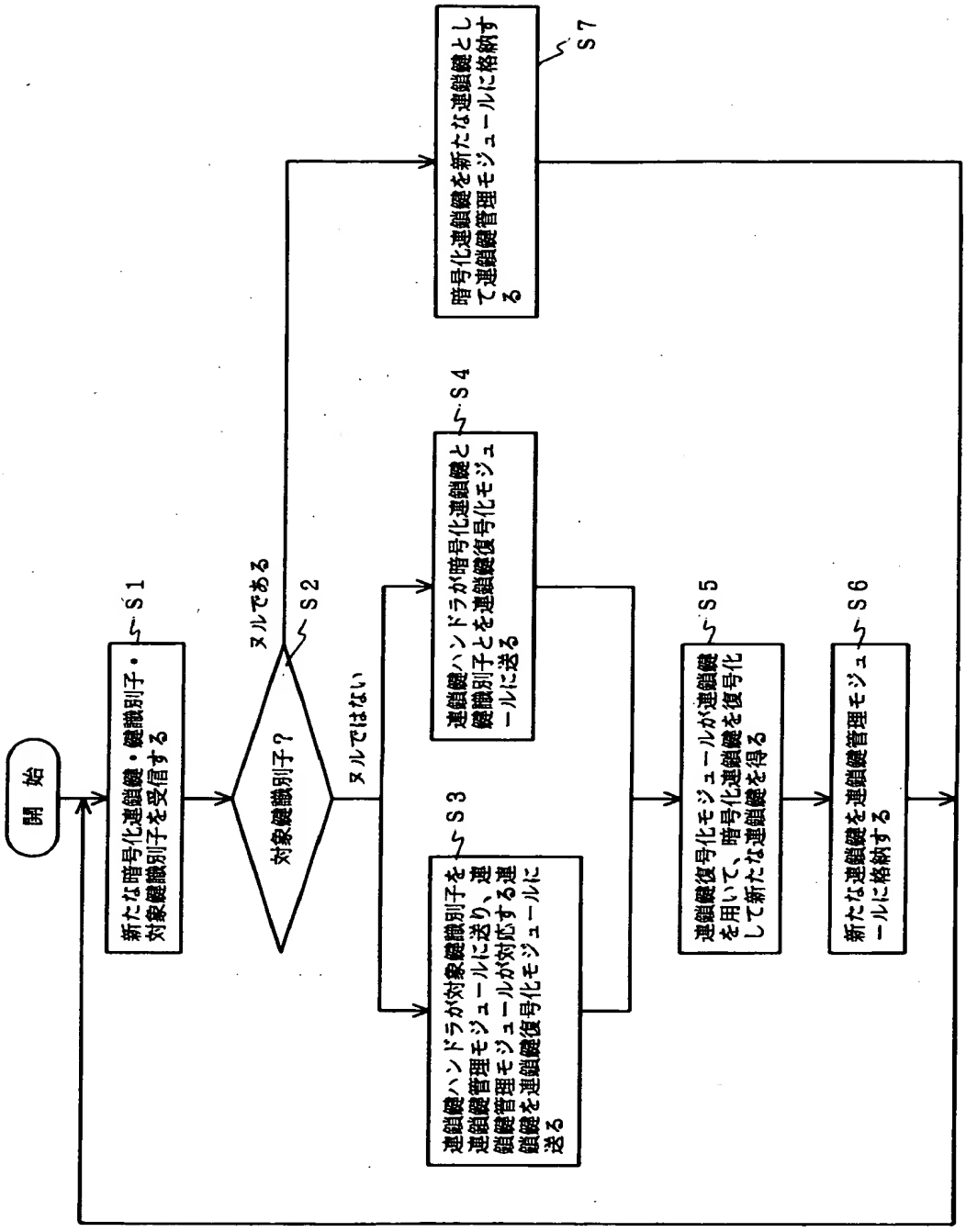
【図２】


放送信号
11
デマックス
MPEGデータ
12
映像デコーダ
映像データ
13
映像モニタ
暗号化連鎖鍵
鍵識別子
対象鍵識別子
連鎖鍵ハンドラ
14
暗号化連鎖鍵
鍵識別子
15
連鎖鍵
復号化モジュール
連鎖鍵
鍵識別子
暗号化連鎖鍵
鍵識別子
対象鍵識別子
連鎖鍵管理モジュール
16
連鎖鍵メモリ
18
鍵識別子
連鎖鍵
17
コンテンツ
復号化モジュール
ハードディスク
19
復号化
コンテンツ

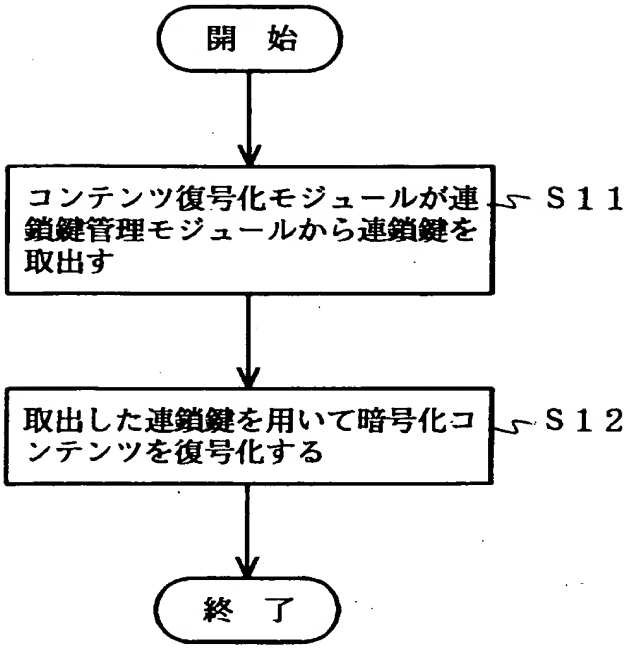
【図３】


鍵識別子＃１
連鎖鍵＃１
鍵識別子＃２
連鎖鍵＃２
鍵識別子＃３
連鎖鍵＃３
鍵識別子＃４
連鎖鍵＃４
鍵識別子＃５
連鎖鍵＃５
連鎖鍵メモリ
１８

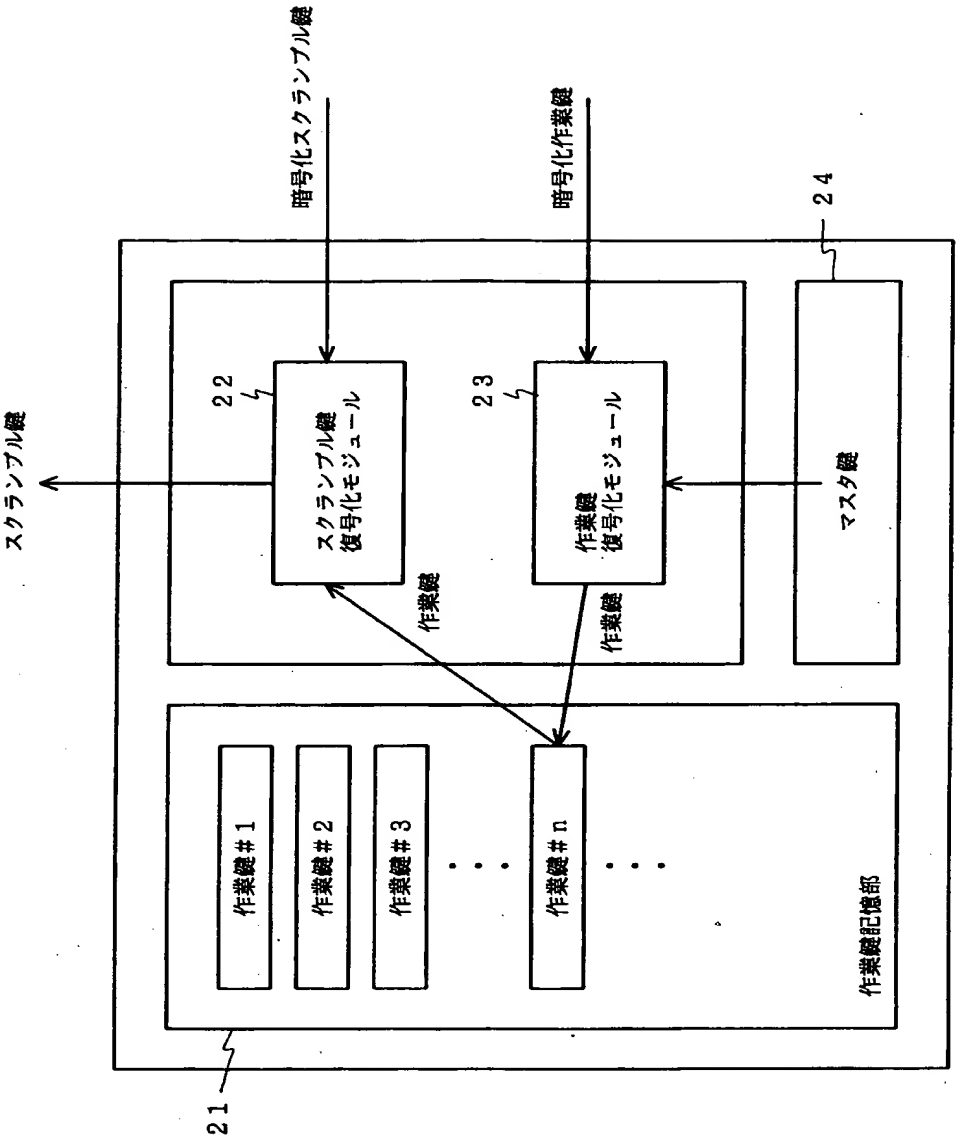
【図４】


開 始
新たな暗号化連鎖鍵・鍵識別子・対象鍵識別子を受信する
S1
対象鍵識別子？
S2
ヌルである
ヌルではない
連鎖鍵ハンドラが対象鍵識別子を連鎖鍵管理モジュールに送り、連鎖鍵管理モジュールが対応する連鎖鍵を連鎖鍵復号化モジュールに送る
S3
連鎖鍵ハンドラが暗号化連鎖鍵と鍵識別子とを連鎖鍵復号化モジュールに送る
S4
連鎖鍵復号化モジュールが連鎖鍵を用いて、暗号化連鎖鍵を復号化して新たな連鎖鍵を得る
S5
新たな連鎖鍵を連鎖鍵管理モジュールに格納する
S6
暗号化連鎖鍵を新たな連鎖鍵として連鎖鍵管理モジュールに格納する
S7

【図５】


開　始
コンテンツ復号化モジュールが連鎖鍵管理モジュールから連鎖鍵を取出す
Ｓ１１
取出した連鎖鍵を用いて暗号化コンテンツを復号化する
Ｓ１２
終　了

【図６】


暗号化スクランブル鍵
暗号化作業鍵
24
22
23
スクランブル鍵
スクランブル鍵
復号化モジュール
作業鍵
復号化モジュール
マスタ鍵
作業鍵
作業鍵
作業鍵＃1
作業鍵＃2
作業鍵＃3
作業鍵＃n
作業鍵記憶部
21

【書類名】　　要約書

【要約】

【課題】　復号化した鍵を次回以降の復号に用いる処理が実現可能な連鎖鍵放送システムを提供する。

【解決手段】　連鎖鍵受信手段１は連鎖鍵、その鍵識別子、及びその鍵が復号化する連鎖鍵を示す対象鍵識別子を受信する。連鎖鍵保存手段３は連鎖鍵受信手段１で受信した対象鍵識別子を用いて既に保存されている連鎖鍵を取出す。連鎖鍵復号化手段２は連鎖鍵保存手段３から送られてくる連鎖鍵を用いて、連鎖鍵受信手段１が受信した連鎖鍵を復号化して新たな連鎖鍵を生成する。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００４２３７〕

１．変更年月日　　１９９０年　８月２９日
［変更理由］　新規登録
住　所　東京都港区芝五丁目７番１号
氏　名　日本電気株式会社